Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 32

12-24-2024

Digital Twin and Cybersecurity in Additive Manufacturing

Lidong Wang
Mississippi State University, lidong@iser.msstate.edu

Recommended Citation
Wang, Lidong (2024) "Digital Twin and Cybersecurity in Additive Manufacturing," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 32.
DOI: https://doi.org/10.62915/2472-2707.1201
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/32

Digital Twin and Cybersecurity in Additive Manufacturing

Abstract

Additive manufacturing (AM) has been applied to automotive, aerospace, medical sectors, etc., but there are still challenges such as parts' porosity, cracks, surface roughness, intrinsic anisotropy, and residual stress because of the high level of thermal gradient. It is significant to conduct the modeling and simulation of the AM process and achieve quality products. Digital Twin (DT) can help AM with forecasting defects/errors through simulation and real-time process monitoring. DT is a concept of Industry 4.0, and its digital structure reflects the real-time behaviors of a cyber-physical or physical system. This paper introduces the progress of DT applications in AM, cyber digital twin (CDT), cybersecurity digital twin, and cybersecurity in AM, and highlights the challenges of DT and cybersecurity in AM. A case study is presented, including the flaw formation of laser powder bed fusion (LPBF) due to cyber intrusions and the flaw formation during the printing process of LPBF, the impacts of the factors of cyber resilience on the AM supply chain, and cyberattacks on various data categories of AM and their business impacts. The methods and related information in this paper not only help promote professionals' research and development in the industry, but also are very useful for faculty's research and teaching as well as students' learning in the areas of DT, AM, and cybersecurity.

Keywords

digital twin, cybersecurity, additive manufacturing (AM), artificial intelligence (AI), machine learning (ML), blockchain, cyber digital twin (CDT)

Cover Page Footnote

The author would like to thank the support from Mississippi State University.

Digital Twin and Cybersecurity in Additive Manufacturing

Lidong Wang
Institute for Systems Engineering Research
Mississippi State University
Mississippi, USA
lidong@iser.msstate.edu
ORCID: 0000-0002-5071-3311

***Abstract*—Additive manufacturing (AM) has been applied to automotive, aerospace, medical sectors, etc., but there are still challenges such as parts' porosity, cracks, surface roughness, intrinsic anisotropy, and residual stress because of the high level of thermal gradient. It is significant to conduct the modeling and simulation of the AM process and achieve quality products. Digital Twin (DT) can help AM with forecasting defects/errors through simulation and real-time process monitoring. DT is a concept of Industry 4.0, and its digital structure reflects the real-time behaviors of a cyber-physical or physical system. This paper introduces the progress of DT applications in AM, cyber digital twin (CDT), cybersecurity digital twin, and cybersecurity in AM, and highlights the challenges of DT and cybersecurity in AM. A case study is presented, including the flaw formation of laser powder bed fusion (LPBF) due to cyber intrusions and the flaw formation during the printing process of LPBF, the impacts of the factors of cyber resilience on the AM supply chain, and cyberattacks on various data categories of AM and their business impacts. The methods and related information in this paper not only help promote professionals' research and development in the industry, but also are very useful for faculty's research and teaching as well as students' learning in the areas of DT, AM, and cybersecurity.**

Keywords*—digital twin, cybersecurity, additive manufacturing (AM), artificial intelligence (AI), machine learning (ML), blockchain, cyber digital twin (CDT)

I. Introduction

Huge multimodal data are produced and utilized throughout an AM lifecycle, from material design, part design, and simulation to part printing, post-processing, and inspection. A federated and multimodal (big) data storage and analytics platform was developed to link and capture various data. It included the following tiers: 1) the distributed polyglot data storage and analytics tier with various repositories (used for data with structures), 2) the metadata knowledge graph tier (used for the modeling of datasets and their relationships among the repositories), and 3) the user interface tier (used for the visualization, exploration, and analytics of the data) [1].

The primary benefits of metal AM in the aerospace sector are the reduction of lead time and costs. In addition, mass reduction is a major advantage through optimizing design or using multiple alloys. There are many opportunities for metal AM in aerospace, including novel materials, unique design, the consolidation of multiple components, the mass reduction of components (due to lightweight designs), further lead-time and cost reduction, etc. These opportunities are being employed in aerospace such as satellite components, liquid-fuel rocket engines, and turbomachinery. AM has challenges especially in the aerospace industry, including potential reduced fatigue properties, limited materials for utilization, possible unique quality control requirements, post-processing, the certification of parts, expertise required for manufacturing some functional components, etc. [2].

Augmented reality (AR) is a technique of augmenting real objects with extra digital information. The combination of the AR and DT techniques has a noteworthy impact on cybersecurity, particularly on the cybersecurity of cyber-physical systems (CPS). Some benefits could be fulfilled with AR-driven DT. Manufacturing is a popular area of the AR-DT combination. More tools could be employed to ensure enough confidentiality, integrity, and availability (CIA) for the combination of the AR and DT techniques. The security tools or techniques can be used in data encryption, access control, and secure synchronization between an AR-driven DT and a physical system. Enhancing cybersecurity particularly depends on the continuous tracking of physical and virtual/digital objects and the characteristics of the continuous data flow. The continuous tracking may need anonymization or encryption methods to guarantee the privacy of an end user. The data flow also needs secure synchronization and even data encryption techniques [3].

AR helps get augmented maintenance manuals and parts catalogs. AM can be utilized in remote maintenance, where real-time virtual/digital animations can be ready. AR and AM enable a better way to perform maintenance operations compared with a conventional technique. AM helps avoid a big warehouse and simplify the supply chain. AR provides an operator with user-friendly manual(s) where instructions and virtual/digital models are combined with the real world. AR can also work together with AM: a practitioner identifies a failed part utilizing AR, then the part can be virtually extracted utilizing reverse engineering techniques, and finally, it is sent to an AM machine to print [4].

The primary purpose of the research in this paper is to deal with DT, AM, and cybersecurity; present the recent advances and progress in the three interdisciplinary areas; and promote cybersecurity education, research, and practice, including not only professionals' research and development in the industry, but also faculty's research and teaching as well as students' learning in the areas of DT, AM, and cybersecurity. The remainder of this paper will be organized as follows: the second section is the research methodology of this paper; the third section introduces DT and cybersecurity; the fourth section presents DT in AM, the fifth section introduces DT with blockchain and AI/ML in AM; the sixth section presents cyber digital twin and cybersecurity digital twin; the seventh section provides a case study, including the flaw formation of laser powder bed fusion (LPBF) due to cyber intrusions and the flaw formation during the printing process of LPBF, the impacts of the factors of cyber resilience on the AM supply chain, and cyberattacks on various data categories of AM and their business impacts; and the eighth section is the conclusion.

II. Research Methodology

Literature research was conducted using the database EBSCO via 'Advanced Search' to search papers on "digital twin" and "cybersecurity", "digital twin" and "additive manufacturing", "digital twin" and "3D printing", "cybersecurity" and "additive manufacturing", "cybersecurity" and "3D printing", "digital twin" and "artificial intelligence", "digital twin" and "machine learning", "digital twin" and "blockchain", "additive manufacturing" and "artificial intelligence", "additive manufacturing" and "machine learning", "additive manufacturing" and "blockchain", "3D printing" and "artificial intelligence", "3D printing" and "machine learning", and "3D printing" and "blockchain". 'Subject Terms' was selected as 'Field' in the EBSCO database for searching papers. Targeted papers were published between January 2017 and October 2024 in English and scholarly (peer-reviewed) journals or conferences. Duplicated papers and weak papers were removed. The number of quality papers selected for the literature review is 148, but only 52 papers were cited in this paper because the papers matched the topics and the research objectives of this paper.

There are the following research questions for the study in this paper:

1) What are the advantages of DT?
2) What are the development steps of DT?
3) What are possible cyberattacks during the development steps of DT?
4) What are the key technologies that promote DT?
5) What are the recent developments of DT for AM (3D printing)?
6) What are the challenges in creating a DT system of AM?
7) What cybersecurity issues are in DT and AM?
8) How do blockchain and AI/ML promote DT and AM and enhance their cybersecurity?
9) What are strategies or potential solutions to overcome challenges in DT, AM, and cybersecurity?
10) What are the approaches (qualitative, quantitative, or hybrid) to assessing the impacts of cyberattacks on AM?
11) Is there any empirical evidence in published papers that can be used to develop a case study in DT, AM, and cybersecurity?

The following sections will focus on the above research questions; investigate recent and relevant studies in DT, AM, cybersecurity, AI/ML, and blockchain; find what has been conducted or published; provide the details of the research related to the questions, discuss the limitations of this paper, and outline the topics of future research. The topics in this paper are interdisciplinary with values in cybersecurity education, research, and practice. New and potential research questions or issues are coming out with the research progress and advances in DT, AM, and cybersecurity. New pillar technologies (besides AI/ML and blockchain) are expected to support the research of these topics.

III. Digital Twin and Cybersecurity

DT is a concept of Industry 4.0. It means a digital and informational construct reflects the behaviors of an observable CPS or a physical system in a real-time modeling and simulation situation [5]. A DT is a multi-physics simulation that is connected to its real counterpart (such as a product, machine, or plant) directly through interfaces, sensors, and electronic control systems. A DT offers the following advantages [6]:

- Working variables/parameters monitoring and automated management of data flow.
- Real-time/online or offline optimization of working settings.
- Prediction as well as prevention of machine errors.

A DT permits real-time monitoring, assessment, automated control process, and the change of building parameters as needed. A DT enables the optimization, simulation, prediction, and monitoring of a CPS. It is necessary to guarantee that a DT can protect the identity of its true twin [7]. One approach to enhancing cybersecurity is employing DT to perform security testing. A DT needs to be flexible and has the capability of 1) being switched on or off as needed; 2) integrating new software components easily; and 3) modifying easily according to the connectivity architecture. An architecture of managing flexible and on-demand execution of DT was presented based on the telecom-oriented network functions virtualization. The DT can perform the testing of possible cyber risks/threats as well as associated countermeasures [8].

Researchers proposed a framework of DT for detecting cyberattacks in cyber-physical manufacturing systems. A case study on off-the-shelf AM printers was presented using experimental cases to identify cyberattacks employing the framework to demonstrate the efficacy of the proposed method. The presented DT utilizes physics-based models, data-driven ML models, and professional knowledge to detect cyberattacks [9].

Table I shows DT and its development steps [10][11]. Possible cyberattacks during the steps are as follows: 1) stored data attacks, node capture, and false injection of sensor data during data collection; 2) denial of service (DoS), sniffing, and man-in-the-middle (MitM) during data transmission; 3) data manipulation, unauthorized attack, and SQL injection during

TABLE I. DT AND ITS DEVELOPMENT STEPS

Aspects	Description
Definition	Virtual/digital representation (real-time) of a physical object or process.
Features	Reprogrammable, enhanced connectivity, modularity, and data homogenization.
Major components	Physical, virtual/digital entities, & their connections.
Benefits	Faster production, predictive maintenance, risk evaluation, real-time decision-making
DT development steps	• Data collection ➢ Real-time & operational data are collected by sensors, then sent to a micro-controller for aggregation or further processing; the processed data are sent back to the actuator for instant action (if needed) or are sent to the next step. • Data transmission ➢ The processed data is transmitted to the next step via Wi-Fi or 5G network. • DT generation ➢ The received data are saved in data repositories (data warehouses or lakes) and analyzed based on methods such as ML/DL to create the DT of the physical entity. • DT visualization ➢ The generated DT is visualized and can be evaluated.

DT generation; and 4) phishing, session hijacking, and cross-site scripting during the DT visualization.

DT pillar technologies include data networks, the Internet of Things (IoT), sensors, data visualization, simulation/emulation, AI, and cloud computing [12]. DT is an enabling technology promoting the development of intelligent manufacturing. Specific technologies and details that promote DT in this area are listed in Table II [13].

The security of a CPS relies on sensor network security. Most work regarding sensor network security in the past focused on planning a secure communication infrastructure. Consequences include effectual algorithms for: 1) bootstrapping security association and key management to create a secure infrastructure; 2) secure communications; and 3) secure routing protocols. Possible sources of information to reveal virtual objects can be network communications, log documents, and sensor estimates from actual/physical objects. Creating a layer for cybersecurity within a DT is a challenge. A DT needs to enable the security of the identity and the protection of its genuine twin, which requires the utilization of algorithms in cryptography [14].

A CPS includes physical and cyber components. A DT is a clone (cyber nature) of physical components, and it is basic in a CPS. Using a DT can also introduce problems of security in Industry 4.0. A space of attacks in a DT-based CPS and defenses were introduced with the consideration of various layers and attack objects (confidentiality, integrity, and availability), which is listed in Table III [15, 16, 17]. A defense mechanism was proposed. It is also important to leverage other methods (blockchain, intrusion detection, etc.) to secure the DT-based CPS [15].

TABLE II. TECHNOLOGIES PROMOTING DT

Technologies	Details
Data acquisition & transmission technology	• Multi-sensors • Layout network of multi-sensors • Data fusion of multi-sensors • Radio frequency identification (RFID) • Data acquisition boards • IoT • Embedded systems • 5G • High broadband • Communication protocols • Transmission interfaces • Network of data transmission • Platforms of data transmission
Data management technology	• Data screening • Data cleaning • Unified identification of unstructured data • Value evaluation/assessment • Value correlation of multi-source data • Feature extraction • Distributed cloud-storage service systems
Intelligent algorithm & computing power	• Validation of algorithms • Optimization of algorithms • Algorithm-fusion guide • Patterns of distributed computing • Platforms of cloud computing
DT modeling technology	• 3D-scanning • Derivative design • Knowledge maps • Unified modeling language • Model-driven architecture • ML • Lightweight of models • Mechanisms of model-evaluation • Comparison of models • Functional mock-up interface • Functional mock-up units
Human-computer interaction technology	• Virtual reality • AR • Mixed reality • Voice recognition • Behavior-image recognition • Platforms for multi-user collaboration • Reverse algorithms • Technology of model-evaluation

IV. DIGITAL TWIN IN ADDITIVE MANUFACTURING

DT enables the integration of cyberspace and physical space; therefore, it is well-fitted to AM because it can benefit from digitized assets and data analytics for process control [17]. AM is a digitized process; therefore, it is convenient to use the concept of DT. DT helps enhance the process performance of AM regarding the roughness, porosity, deformation, defects, etc. [19]. DT is a CPS with the virtual existence of a twin of a physical object. It is defined as a system with five components, which include services, connections, DT data, virtual entities, and physical entities. Bidirectional communication is important because it permits a virtual entity to communicate with a physical entity and vice versa. AM is suitable to use DT or collaborate with it because AM itself is digital throughout the whole manufacturing lifecycle. The digital nature of AM indicates that there is much interconnecting data captured and

TABLE III. ATTACKS IN VARIOUS LAYERS TOWARDS SMART MANUFACTURING AND DEFENSES

Layers	Examples of Attack Types	Description of Attacks	Cybersecurity Objectives	Defenses
Object layer	Eavesdropping	Gaining sensitive information regarding the behaviors of a sensor through monitoring the network of manufacturing.	Confidentiality	Sensor authentication and validation (for original sensors without being tampered with)
	Spoofing	Getting illegitimate access to actuators, sensors, & controllers during the manufacturing process.	Integrity	
	DoS	Preventing the data of sensors in manufacturing from reaching their destinations & making data unavailable.	Availability.	
Communication layer	Spoofing	Compromising the confidentiality of the manufacturing system.	Confidentiality	Cryptography for the trustworthiness & security of transmitted data; antivirus, firewalls, & intrusion detection systems for securing DT from internal & external attacks/threats.
	MitM	Sensitive data in manufacturing can be captured and modified by adversaries.	Integrity, Confidentiality	
	Sinkhole	Undermining the availability or secrecy of systems.	Availability, Confidentiality	
	DoS	Shutting down instance communications in a control loop by disrupting the on-demand supply of data.	Availability	
DT layer	MitM	Causing manufacturing defects by altering the data of manufacturing captured before reaching a DT model.	Integrity	Data encryption & secure transmission for the protection of the DT resources (e.g., AI data & model); regular vulnerability assessment.
	Data injection	Inserting data into a model (e.g., AI model) of a DT & causing a machine to misbehave.	Integrity	
	DoS or distributed DoS (DDoS)	Disrupting the production of goods & services.	Availability	
Application layer	Phishing	Disclosing confidential information regarding the manufacturing system.	Confidentiality	Authentication, software with security standards, software hardening, anomaly detection, etc.
	Malicious virus/worm	Cause malware propagation & endangering manufacturing services.	Availability	
	Malicious scripts	Disrupting manufacturing applications.	Availability	

stored throughout every step of the AM process. This can also be called the AM digital thread. Therefore, DT can run with the AM digital thread in parallel, using available data to perform analytics and modeling/simulation [20].

A DT is the computerized model of a physical object, assembly, or system that is updated based on the data that is captured from its physical twin [21]. DT is a potential approach to overcoming challenges (e.g., process monitoring, simulation, and control) in AM [22]. In-situ monitoring and accurate identification of flaws using DT have been one of the important research areas of AM [2]. Additive layer manufacturing can introduce defects, for example, cracking, porosity, residual stress, and high surface roughness. DT helps to predict errors and mitigate them by process monitoring and simulation in real-time, especially in the aerospace industry [12]. A method of using AR was introduced to communicate the layout information between a reconfigurable AM system and its DT for the toolpath simulation and planning [23]. A dynamic system that represents an AM process needs to be developed under one or more factors as follows: noise, disturbance, uncertainty, and delay. A DT with robust process control and uncertainty management was created and fulfilled, which demonstrated that DT could help the AM process control [24].

AM technologies include fused deposition modeling (FDM), direct energy deposition (DED), powder bed fusion (PBF), laser-engineered net shaping (LENS), laser sintering (LS), laser metal deposition (LMD), fused filament fabrication (FFF), wire arc additive manufacturing (WAAM), etc. Approaches to promoting DT development in AM include the finite element method (FEM), ML, AR, cloud, IoT, digital image processing, etc. Some recent DT development in AM is shown in Table IV [25].

TABLE IV. SOME DEVELOPED DTS IN AM

Capabilities	Objectives	AM Technologies	Approaches
Predictive	Simulate the process of printing	Metal AM	FEM
	Predict the efficacy and performance of manufacturing	FDM	Build time model
	Forecast the properties of products and decide the relationship between outputs and inputs	DED	FEM
		PBF	FEM
		LENS	FEM
		FDM	FEM, ML, Optical simulation tool
Diagnostic and control	Simulation-based process control & process planning	FDM	AR, Cloud
	Real-time control based on sensors	Framework	Cloud, IoT
			Cloud, ML
Supervisory	Product life-cycle monitoring	FDM	AR
		PBF	QR codes
		LS, FDM	Blockchain
	Monitoring of molten-pools	PBF	DIP, FEM, ML
		LMD	DIP, FEM, ML
		PBF, DED	FEM, DIP, ML
	System status monitoring	FFF	FEM
		FDM	IoT
	Defects & faults monitoring	FDM	ML, IoT
		WAAM	ML

A DT ecosystem was developed to perform process monitoring, testing, and remote management of FDM machines in a simulated or virtual environment. The components of the DT ecosystem and the functions or tasks of each component are shown in Table V [5]. A DT of AM enables the forecast of temporal and spatial variations of metallurgical variables/parameters that influence components' properties and structures. Building blocks for developing a DT of laser-based DED utilize a transient 3D model that computes cooling rates, temperature and velocity fields, solidification variables/parameters, and deposit geometry [26].

A method of DT-driven and collaborative data management for metal AM systems was proposed, which is shown in Table VI [27]. There are six modules in the framework, including a collaborative data management module based on the cloud and five modules that represent five product lifecycle stages, respectively. It is not efficient or even possible to transfer all field-level data to a cloud to establish a DT; therefore, each lifecycle stage has an edge DT that focuses on local tasks and transfers the processed data to a cloud DT for various applications and users [27].

Laser PBF (LPBF) is an AM technology. There are three pathways to flaw formation in LPBF parts: 1) machine-related malfunctions (lens delamination); 2) changes in the processing variables/parameters (due to process drifts); and 3) deliberate tampering with the process or planting flaws in a part to compromise its performances, which is cyber intrusion. Cybersecurity is an emerging concern in LPBF. A DT strategy for the in-situ detection of flaws in the LPBF process was demonstrated [28]. There are challenges regarding DT implementation in AM [19]:

- The physical status of AM is dynamic (with constant change) owing to the interaction with the environment. Predicting the interaction and environmental impact is crucial, but not easy.
- Process control with a closed loop is important. A cloud system and an effective IIoT (Industrial IoT) are needed.
- Lack of standardization of definition, interoperability, interface, control, and integration in the cyber and physical manufacturing system.

WAAM has been gradually recognized because of its fabrication capability of large-scale parts. A DT execution structure for WAAM was proposed [18]. WAAM permits the customized and economical production of metal parts on a large scale. It is categorized as DED. During the build-up procedures, defects (e.g., pores, oxidations, delamination, burn-throughs, and geometrical deformation) can happen because of process instability or inappropriate process parameters. The defects destroy the part quality. Research on context-aware monitoring was conducted based on the integration of spatial, temporal, and machine context in data analytics. Creating a DT of produced parts utilizing an Octree as a data structure for spatial indexing enables the awareness of spatial contexts. Two metrics of quality (the local anomaly density and the defect expansion) were presented. Defects were found in the process with high sensitivity, showing less false negatives and false positives [29].

TABLE V. A DEVELOPED DT ECOSYSTEM FOR FDM

Components	Functions or Tasks
Component of data acquisition-processing-distribution	• Data acquisition • Data processing • Data distribution • Data storage
Component of virtual representation	• 3D simulations • Extended reality • "What if" analysis • Monitoring • Reports

TABLE VI. DT-DRIVEN AND COLLABORATIVE DATA MANAGEMENT FOR METAL AM

Modules	DT Types	Targets Supported by DTs	Functions or Tasks of DTs
Collaborative data management	Cloud DT	• Data analysts • Project managers • Customers • Data analytics tools	• Metal AM product data models • Product lifecycle data • Cloud database • Advanced data analytics • Application interfaces
Product design	Edge DT	• Product designers • CAD/CAE software	• Product design files • CAE simulation • Design optimization • Local database
Process planning	Edge DT	• Process planners • CAM software	• Support structure design • Process planning • Process simulation • Process optimization • Local database
Manufacturing	Edge DT	• Metal AM machines • Machine operators • Process monitoring systems	• Real-time data processing • Process monitoring • ML model training • In-process quality control • Decision-making support • Local database
Post-processing	Edge DT	• Post-processing machines • Machine operators • Process monitoring systems	• Process simulation • Process monitoring • Machine control • Process optimization • Local database
Quality measurement	Edge DT	• Machine operators • Quality measurement devices	• Device control • Data processing • Result analysis • Report generation • Local database

TABLE VII. CHALLENGES IN CREATING A DT SYSTEM OF WAAM

Categories/ Aspects	Challenges
Deposition modeling	• Volumetric change due to a phase transformation, the creep strain of a material, & transformation-induced plasticity. • The model of fatigue & corrosion behaviors. • The fluid flow of the molten pool & its effect on the thermal history & deposition geometry. • The spatter formation in a consumable welding process. • The shielding gas influence as a function of welding variables/parameters & its effect on the molten pool. • The relationship/correlation of manufacturing process parameters, microstructure, & generated defects. • Instability due to the welding arc blow. • The model of the tool health (e.g., the wear mechanism of an electrode in a consumable welding process).
Scalability and efficiency	• Lack in the formation process control, e.g., microstructure, distortion, and residual stress. • The planning, simulation/modeling, and control strategy for a complex structure should be optimized to manage the filling path, thermal behaviors, distortion, residual stress, surface quality, computing efficiency, etc. • Lack of databases that include various deposition materials. • A multi-physics and multi-scale system needs to be established for the improvement in the scalability of the system and the reduction of experiments. • The reduction of computational time, hence the fulfillment of AI/ML, cloud computing, etc.
Process integration	• Non-destructive testing for monitoring product quality, fusion of in-process sensors, & integration of hardware. • Pre-processing • Post-processing • In-situ processing
Digitalization	• Data transmission efficiency • Data traceability and transparency/visibility

Although WAAM has attracted attention, there are challenges in creating a DT system of WAAM and the challenges are categorized into four categories (aspects) that are listed in Table VII [25].

V. DIGITAL TWIN WITH BLOCKCHAIN AND AI/ML IN AM

The integration of DT, CPS, and cutting-edge technologies (such as IoT, AI/ML, cloud computing, and Big Data analytics) has become a pillar of Industry 4.0 (the fourth industrial revolution). DT has been used for anomaly detection in manufacturing. DT creates new chances in fault prognosis, fault detection and diagnosis, and condition monitoring for anomaly detection. DT can monitor and display the difference or deviation between the expected values and the collected data; therefore, it can detect anomalies according to performance metrics [30].

Metal AM requires a DT that can tackle the issues of printed part qualification, certification, and optimization. Crucial technologies are hardware control systems, in-situ sensing, surrogate modeling, and intelligent control policies. A DT of metal AM with four levels was proposed, which is shown in Table VIII [31].

TABLE VIII. A DT OF METAL AM

Layers	Description
Implicit	Model/visualize an AM machine, its print geometries, as well as its printing processes.
Instantiated	Observe a physical system with sensors as well as utilize the model prediction.
Interfaced	Modulate the AM system (physical) based on the data of sensors and the model prediction.
Intelligent	Autonomous optimization of print parameters using AI.

Topology optimization in AM is important in creating a compliant system with good performance. DT and AR have worked with topology optimization for improved design collaboration and visualization. The convergence of IoT, cloud computing, and Big Data analytics promotes the advancement of the digital triad (combining digital threads, DTs, and digital trust) as well as secure data sharing, but data security and privacy are still a major concern. Using ML for cyberattack detection or mitigation and secure frameworks based on blockchain technology for intellectual property (IP) management have been recommended for reducing cyber risks in an AM system. The possibility of the integration of DTs with topology optimization that can simulate the behaviors of a complete manufacturing system was studied [32].

A framework of DT based on blockchain was proposed as trusted twins for securing CPS. By leveraging blockchain with DTs, an accountable entity for updating or adding security and safety rules can be tracked and the reliability of data generation sources can be guaranteed through the integrity checking mechanism [33]. Blockchain helps ensure information integrity through the consensus and trust mechanism. It has been used in manufacturing. The application of DT combined with blockchain for manufacturing collaboration and data sharing was discussed. A method of data management was proposed utilizing blockchain. The application of blockchain integrated with physically unclonable functions was introduced in integrated circuits (ICs) to detect counterfeit ICs in the supply chain [34]. A framework based on blockchain, DT, and AM in the context of Industry 4.0 for customer-oriented or personalized manufacturing was proposed [35]. A DT for AM in the aircraft sector based on blockchain was proposed. A conceptual solution to organizing and securing the data from the end-to-end AM process was provided [36].

Explainable AI (XAI) was studied based on cybersecurity modeling through a taxonomy of AI and XAI methods that help in understanding system functions, detecting anomalies and possible risks, and dealing with them in DT situations. The explainability of AI is based on model transparency, the usage realm (such as global, cohort, and local models), working stages (pre-modeling, in-modeling, and post-modeling), and model specificity, including specific model structures such as the architecture of CNN and specific techniques such as decision trees and support vector machine (SVM) [37].

The security of data (in transit or at rest) in DT is a major concern. Encryption and blockchain ensure the integrity and privacy of data, especially sensitive information. AI and its applications, challenges in DT security, proactive cyber defense techniques for DT, comprehensive security tools and strategies for DT, etc. have been investigated, which is shown in Table IX [38].

An approach to the security protection of cyber-physical production systems (CPPSs) was presented by leveraging DT to create a comprehensive model. This approach provides a DT-centered framework and cooperative platform for cybersecurity and manufacturing that helps security assessments (e.g., vulnerable component mitigation prioritization in CPPSs without compromising operations) [39]. Using CPS, AM, and DT, a framework for flexible de- and remanufacturing systems was proposed [40].

A DT framework for a real-time model predictive control of process parameters of laser directed-energy deposition (DED) was presented. A surrogate model using LSTM (long short-term memory)-based ML was developed, which can perform a real-time temperature prediction. A Bayesian optimization method for time series process optimization (BOTSPO) was used to decide suitable laser power profiles for enhancing heat treatment and maximizing the part's precipitation hardening time [41].

TABLE IX. AI, DT, AND DT SECURITY

Aspects	Details
Main AI advantages in DT cybersecurity	• Fast threat detection • Quick response • Automating routine work • No human errors
Main AI disadvantages & major cybersecurity challenges in DT	• Hackers are also AI-savvy • Dynamic threats • Cyberthreats continue to evolve • Heterogeneity/scale (various hardware/software designs & local policy areas) • Distanced infrastructure (sending sensitive data around the globe, inadequate protection)
Attack methods by AI in DT	• Automated detection of vulnerabilities used by cybercriminals • False data injection and poisoning • Fuzzing technique (feeding designed inputs to a program to trigger vulnerabilities & cause a system to crash)
Proactive cyber defense techniques for DT	• Enhanced simulation & modelling • Threat intelligence sharing • Penetration testing & red teaming • Anomaly detection using ML
Comprehensive security tools & strategies for DT	• AI/ML • Blockchain • Encryption • Vulnerability assessment tools • Cybersecurity awareness training • Authentication and access control • Regular security assessment & penetration testing • Advanced threat detection & response systems • Identity & access management (IAM) systems • Secure development life cycle (SDLC) • Security information and event management (SIEM) systems • Network security using firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), or intrusion detection & prevention systems (IDPS)

Federated learning generally utilizes various customers to implement a training process to protect their privacy. It is more efficient for a manufacturer with various branches to participate in the training of federated learning as one group. DT enables efficiency for the communication between physical assets and digital assets to perform seamless information processing. It is often built with the following layers: field devices, edges, platform(s), and applications. A federated learning architecture that enabled DT for AM was introduced. A model based on the convolutional neural network (CNN) was proposed to learn the data of sensors of an AM printer for fault detection. A platform of DT was created for monitoring and control. The platform can initiate, monitor, and stop the AM process through a digital/virtual environment [42].

VI. Cyber Digital Twin and Cybersecurity Digital Twin

A DT is a virtual/digital representation of a physical object. DT has been achieving impetus in cybersecurity. Its primary applications and advantages lie in the capability of attack modeling/simulation and the assessment of countermeasures without physical system disruption [43]. DT has been playing a substantial role in handling the following challenges in cybersecurity [3, 44]:

- Improved risk management: DT can improve risk management through testing and simulating the influence of configuration changes on the components of security.
- Anomaly detection: DT and digital shadows help improve the runtime verification, an approach to connecting dynamic testing and anomaly detection.
- Active cyber defense: DT provides an incident responder with knowledge to evaluate cyberattacks.
- Ensuring autonomy: DT helps develop autonomous systems with the potential to respond to anomalies, cyber threats, etc.
- Enhanced security patch management: Using DT in simulating the operation technology infrastructure helps improve security patch management.
- Virtual commissioning: A DT is a performance enabler due to the fault prediction and the virtual commissioning capability.
- Increased security testing opportunities: A cyber digital twin (CDT) is helpful in the testing of security operations. DT and CDT help the providers of services with a full evaluation of possible cyberattacks or vulnerabilities.

Using DTs has raised cybersecurity concerns. DTs themselves also need to mitigate cyber risks. A CDT helps users employ the tools of automation and AI to defend the physical infrastructure. CDT is the application of DT for monitoring and security analysis. A CDT helps a security operator with the discovery of vulnerabilities in a real/physical system based on simulation. CDT helps stop cyberattacks due to the capability of prediction as well as the enhanced visibility of the behaviors of physical counterparts [45].

CDT extends the DT concept in representing software objects. CDT focuses on the software that powers itself and the security thereof [46]. CDT is the building block of a secure Industry 4.0 metaverse. It helps to 1) identify mission-critical assets; 2) manage attack surfaces of assets; 3) offer hands-on training; 4) facilitate non-invasive cyber assessments; and 5) act as a prototyping environment and permit the investigation of the impacts of security updates, tools, and the integration of new technologies [47]. All available interfaces, used software libraries, etc. are found automatedly and included in the model underlying a CDT as shown in Table X [46] when a CDT is created. The analysis of the CDT is performed utilizing the methods of pattern recognition to detect potential vulnerabilities based on the software and hardware bill of materials [46].

The cybersecurity digital twin (cybersecurity DT) is described as a virtual model of a system that accompanies its physical counterpart, consumes real-time data possibly, and has adequate fidelity to permit simulation, testing, as well as execution of favorite business continuity plans and security measures. A cybersecurity DT was derived based on a designed cybersecurity view. Verifying preferred properties of security, analyses without much cost, etc. have noticeable influences through building a cybersecurity digital twin [43].

Operating cybersecurity DT enables enterprises to perform analysis of systems and secure them with a minimal effect on the infrastructure [47]. A cybersecurity DT was proposed. It is an enterprise architecture (EA) model of a system aimed at conducting visual threat modeling and simulation for cybersecurity to develop appropriate countermeasures with no outage of the physical infrastructure. In the first step, a cybersecurity view was derived from an existent EA. The cybersecurity DT was derived from the cybersecurity view in the next step [48]. CDT and cybersecurity DT have the potential to build robust cybersecurity for AM.

TABLE X. A CYBER DIGITAL TWIN (CDT) MODEL

Items	Description
Hardware bill of materials	Hardware components & configuration
Network interfaces	Physical communication interfaces (e.g., Bluetooth, Wi-Fi, USB, and Ethernet) and logical communication protocols (e.g., SMS).
Software bill of materials	Names of libraries & used versions—could be the combination of third-party software (commercial), open-source software, etc.
Operating system (OS)	Commercial system (e.g., VxWorks) or open source (Android, Linux).
OS settings	Configurations & settings
Kernel configuration	Enabled modules & settings
OS-level security configuration	OS security configuration (for authentication or other mechanism of security).
Memory management & mapping	The management system of OS memory, its configurations & usage patterns by executables within the firmware.
Credentials of users	Users' names, passwords, etc. for authentication.
Firewall configuration	Built-in firewall configurations & rules.
Application framework	A framework of usage in the firmware & its configuration.
Application programming interfaces (APIs)	Available API sets to utilize & the ones in utilization.
Application configurations	Configurations and settings with influences on security.
Encryption mechanisms & flows	Encryption service & protocols OF communication utilizing encryption, and the utilization by various applications & systems in the firmware.
Encryption keys	Private & public encryption keys are utilized for external/internal access services.
Control & data flow graph representation	Applications code and control & data flows.

VII. CASE STUDY

A. Case I: Flaw formation of LPBF due to cyber intrusions and flaw formation during the printing process of LPBF

Cyber intrusions can be implemented by malicious actors by putting flaws in a part during the design stage or tampering with the manufacturing process [49, 50]. Spherical-shaped voids were embedded in an impeller. Fig. 1 shows the location of the flaws. Digital twins were applied to practical impellers. The thermal history of a flaw-free impeller is predicted using a graph theory before it is printed. The thermal history of a new part was monitored and updated (based on in-situ sensor data) during the 3D printing process, and the flaw formation (due to changes in the processing parameters) was detected [28], as illustrated in Fig. 2. This demonstrated that DT enables the detection of flaw formation of LPBF.

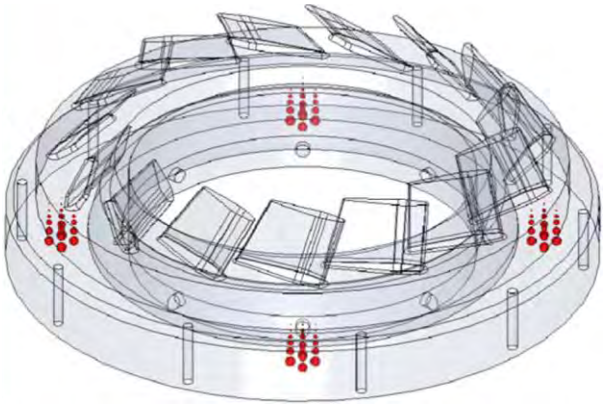

Fig. 1. Voids are embedded into impellers to emulate cyber intrusions [28]

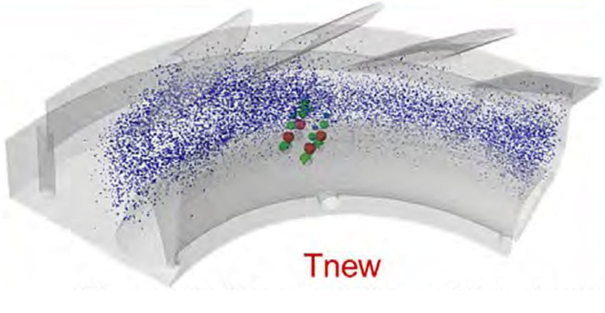

Fig. 2. Thermal history of a flaw-afflicted part [28].

B. *Case II: Impacts of the factors of cyber resilience on the AM supply chain*

There is a high degree of risk in an AM supply chain. It is significant to assess the cyber resilience of the AM supply chain. Factors (attributes) of cyber resilience do not have the same influence on the AM supply chain. It is necessary to evaluate the relative importance of each factor. This can be performed by assigning weights to the factors based on their importance. Analytical hierarchical process (AHP) is an ideal method of weight assignment. It is utilized to rate the cyber resilience factors of the AM supply chain and assign weights to the factors based on collected data. Eight factors of cyber resilience are identified to evaluate the cyber resilience of the AM supply chain. Table XI [51] shows the weights (quantitative approach) for the factors of cyber resilience of the AM supply chain, indicating that confidentiality has the highest weight (0.36) and completeness as well as non-repudiation have the lowest weight (0.04).

C. *Case III: Cyber-attacks on various data categories of AM and their business impacts*

An impact assessment method was used in AM/3D printing. Selected experts from the AM area were interviewed. A numerical value was assigned to the measurement scale adopted (i.e., low impact level = 2; medium impact level = 1; high impact level = 0) in the interviews, and the arithmetic mean (A) of all responses received was computed. The impact levels are determined as follows: it is the high level if the mean (A) is less than 1; it is the low level if the mean (A) is not less than 2; and it is the medium level if the mean (A) is less than 2 and greater than or equal to 1. Table XII [52] shows part of the results, indicating a higher percentage of medium impacts and no low level of impacts. In addition, it is also shown that the most critical security requirement is confidentiality, and the least critical security requirement is availability. This table demonstrates the impacts of cyber-attacks on AM using a hybrid (mixed) approach due to the combination of the qualitative approach (impact levels) and the quantitative approach (mean values).

TABLE XI. WEIGHTS ASSIGNED TO THE FACTORS OF CYBER RESILIENCE OF THE AM SUPPLY CHAIN BASED ON AHP

Factors	**Weights**
Confidentiality	0.36
Integrity	0.20
Availability (access to and use of information in a reliable and timely manner)	0.12
Utility (relevance and usefulness)	0.10
Possession (under control)	0.10
Authenticity (truth, genuine)	0.06
Completeness (sufficiency)	0.04
Non-repudiation	0.04

TABLE XII. AN IMPACT MATRIX WITH IMPACT LEVELS FOR 3D PRINTERS

Data Categories	**Trigger Events**	**Business Impacts**	**Mean (A)**	**Impact Levels**
Product design information	Loss of confidentiality	Reduction in competitive advantage	0.80	High
	Loss of integrity	Product quality degradation	1.40	Medium
	Loss of availability	Loss of production time	1.40	Medium
Machine working parameters	Loss of confidentiality	Reduction in competitive advantage	0.80	High
	Loss of integrity	Product quality degradation	1.00	Medium
	Loss of availability	Loss of production time	1.40	Medium
Workpiece properties	Loss of confidentiality	Reduction in competitive advantage	0.80	High
	Loss of integrity	Product quality degradation	1.20	Medium
	Loss of availability	Loss of production time	1.40	Medium

VIII. CONCLUSION AND FUTURE RESEARCH

DT enables the modeling/simulation, optimization, prediction, and monitoring of the AM process. It is necessary to fulfill the secure identity and the protection of its genuine twin, which must employ cryptography algorithms. CDT is the application of DT to permit process monitoring and security analysis. Various cyberattacks can be simulated to evaluate potential vulnerabilities. Cyberattacks can be malware, DoS, data injection, MitM, etc. DT, especially CDT, helps prevent cyberattacks due to the modeling/prediction capability and enhanced visibility of system behaviors. Utilizing ML to detect and mitigate cyberattacks and blockchain technology to manage IP facilitates the reduction of cyber risks in an AM system. CDT enables vulnerability detection and management as well as security requirements evaluation. Cybersecurity digital twins help analyze and secure systems. CDT and cybersecurity DT have the potential to build robust cybersecurity for AM.

The case study indicates: 1) DT enables the detection of flaw formation of LPBF; 2) for the impacts of the factors of cyber resilience on the AM supply chain, confidentiality has the highest weight, and completeness as well as non-repudiation have the lowest weight; and 3) for cyberattacks on various data categories of AM and their business impacts, the most critical security requirement is confidentiality and the least critical security requirement is availability.

A quantitative approach and a hybrid (mixed) approach to assessing cybersecurity were presented in this paper; however, more advanced assessing methods such as failure mode and effects analysis (FMEA) are required to identify possible cyber threats and failures in complicated situations. Because of the lack of enough experimental data, the capability of ML, especially deep learning (DL) has not been demonstrated adequately. These are the limitations of this paper. For complex and distributed systems in DT, AM, and cybersecurity, effective metrics to detect and prioritize cyber incidents and a holistic approach to handling cyber risks (avoiding risk silos) are significant. Big Data analytics and DL help perform real-time or near-real-time data analytics and cyber risk assessment or prediction, mitigate cyber threats in time, and enhance the cybersecurity of the systems. These are future research topics.

Appendix

TABLE A-I. Acronyms

AM	additive manufacturing
AR	augmented reality
CDT	cyber digital twin
CNN	convolutional neural network
CPS	cyber-physical system
DDoS	distributed denial-of-service
DED	direct energy deposition
DL	deep learning
DoS	denial of service
DT	digital twin
FDM	fused deposition modeling
FEM	finite element method
FFF	fused filament fabrication
LENS	laser engineered net shaping
LMD	laser metal deposition
LPBF	Laser powder bed fusion
LS	laser sintering
MitM	man-in-the-middle
PBF	powder bed fusion
WAAM	wire arc additive manufacturing

Acknowledgment

The author would like to thank the support from Mississippi State University.

Conflicts of Interest

There is no conflict of interest.

Ethics

There is no ethical concern.

References

[1] Aggour, K. S., Kumar, V. S., Cuddihy, P., Williams, J. W., Gupta, V., Dial, L., ... & Vinciquerra, J. (2019). Federated multimodal big data storage & analytics platform for additive manufacturing. In *2019 IEEE international conference on big data (big data)* (pp. 1729-1738). IEEE.

[2] Blakey-Milner, B., Gradl, P., Snedden, G., Brooks, M., Pitot, J., Lopez, E., ... & Du Plessis, A. (2021). Metal additive manufacturing in aerospace: A review. *Materials & Design*, *209*, 110008, https://doi.org/10.1016/j.matdes.2021.110008

[3] Böhm, F., Dietz, M., Preindl, T., & Pernul, G. (2021). Augmented Reality and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity. *Journal of Cybersecurity and Privacy*, *1*(3), 519-538, https://doi.org/10.3390/jcp1030026

[4] Ceruti, A., Marzocca, P., Liverani, A., & Bil, C. (2019). Maintenance in aeronautics in an Industry 4.0 context: The role of Augmented Reality and Additive Manufacturing. *Journal of Computational Design and Engineering*, *6*(4), 516-526, https://doi.org/10.1016/j.jcde.2019.02.001

[5] Pantelidakis, M., Mykoniatis, K., Liu, J., & Harris, G. (2022). A digital twin ecosystem for additive manufacturing using a real-time development platform. *The International Journal of Advanced Manufacturing Technology*, *120*(9), 6547-6563, https://doi.org/10.1007/s00170-022-09164-6

[6] Corradini, F., & Silvestri, M. (2021). A digital twin based self-calibration tool for fault prediction of FDM additive manufacturing systems. Proceedings of the 32nd DAAAM International Symposium, pp.0607-0616, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-33-4, ISSN 1726-9679, Vienna, Austria, doi: 10.2507/32nd.daaam.proceedings.086

[7] Alshammari, K., Beach, T., & Rezgui, Y. (2021, June). Industry engagement for identification of cybersecurity needs practices for digital twins. In *2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (pp. 1-7). IEEE.

[8] Grasselli, C., Melis, A., Girau, R., & Callegati, F. (2023, July). A digital twin for enhanced cybersecurity in connected vehicles. In *2023 23rd International Conference on Transparent Optical Networks (ICTON)* (pp. 1-4). IEEE, doi: 10.1109/ICTON59386.2023.10207369

[9] Balta, E. C., Pease, M., Moyne, J., Barton, K., & Tilbury, D. M. (2023). Digital twin-based cyber-attack detection framework for cyber-physical manufacturing systems. *IEEE Transactions on Automation Science and Engineering*, doi: 0.1109/TASE.2023.3243147

[10] Shaikh, E., Mohammad, N., Al-Ali, A., & Muhammad, S. (2023, January). A probabilistic model checking (PMC) approach to solve security issues in digital twin (DT). In *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)* (pp. 192-197). IEEE.

[11] Mohammadi, N., & Taylor, J. E. (2017). Smart city digital twins. In *2017 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-5). IEEE.

[12] Kozhay, K., Turarbek, S., Ali, M. H., & Shehab, E. (2022, November). Challenges of Developing Digital Twin for Additive Layer Manufacturing in the Aerospace Industry. In *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)* (pp. 1-6). IEEE.

[13] Li, P., Zhu, H., & Luo, L. (2020, October). Digital twin technology in intelligent manufacturing. In *2020 2nd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM)* (pp. 195-200). IEEE, doi: 10.1109/AIAM50918.2020.00046

[14] Alshammari, K., Beach, T., & Rezgui, Y. (2021). Cybersecurity for digital twins in the built environment: Current research and future directions. *Journal of Information Technology in Construction*, *26*, 159-173, doi: 10.36680/j.itcon.2021.010

[15] Hussaini, A., Qian, C., Liao, W., & Yu, W. (2022, August). A taxonomy of security and defense mechanisms in digital twins-based cyber-physical systems. In *2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)* (pp. 597-604). IEEE, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics55523.2022.00112

[16] Al-Ali, A. R., Gupta, R., Zaman Batool, T., Landolsi, T., Aloul, F., & Al Nabulsi, A. (2020). Digital twin conceptual model within the context of internet of things. *Future Internet*, *12*(10), 163, https://doi.org/10.3390/fi12100163

[17] Eckhart, M., & Ekelhart, A. (2019). Digital twins for cyber-physical systems security: State of the art and outlook. *Security and Quality in Cyber-Physical Systems Engineering: With Forewords by Robert M. Lee and Tom Gilb*, 383-412.

[18] Kim, D. B., Shao, G., & Jo, G. (2022). A digital twin implementation architecture for wire+ arc additive manufacturing based on ISO 23247. *Manufacturing Letters*, *34*, 1-5, https://doi.org/10.1016/j.mfglet.2022.08.008

[19] Phanden, R. K., Aditya, S. V., Sheokand, A., Goyal, K. K., Gahlot, P., & Jacso, A. (2022). A state-of-the-art review on implementation of digital twin in additive manufacturing to monitor and control parts quality. *Materials Today: Proceedings*, *56*, 88-93, https://doi.org/10.1016/j.matpr.2021.12.217

[20] Haw, J., Sing, S. L., & Liu, Z. H. (2022). Digital twins in design for additive manufacturing. *Materials Today: Proceedings*, *70*, 352-357, https://doi.org/10.1016/j.matpr.2022.09.268

[21] Scime, L., Singh, A., & Paquit, V. (2022). A scalable digital platform for the use of digital twins in additive manufacturing. *Manufacturing Letters*, *31*, 28-32, https://doi.org/10.1016/j.mfglet.2021.05.007

[22] Kantaros, A., Piromalis, D., Tsaramirsis, G., Papageorgas, P., & Tamimi, H. (2021). 3D printing and implementation of digital twins: Current trends and limitations. *Applied System Innovation*, *5*(1), 7, https://doi.org/10.3390/asi5010007

[23] Cai, Y., Wang, Y., & Burnett, M. (2020). Using augmented reality to build digital twin for reconfigurable additive manufacturing system. *Journal of Manufacturing Systems*, *56*, 598-604, https://doi.org/10.1016/j.jmsy.2020.04.005

[24] Stavropoulos, P., Papacharalampopoulos, A., Michail, C. K., & Chryssolouris, G. (2021). Robust additive manufacturing performance through a control oriented digital twin. *Metals*, *11*(5), 708, https://doi.org/10.3390/met11050708

[25] Mu, H., He, F., Yuan, L., Commins, P., Wang, H., & Pan, Z. (2023). Toward a smart wire arc additive manufacturing system: A review on current developments and a framework of digital twin. *Journal of Manufacturing Systems*, *67*, 174-189, doi: 10.1016/j.jmsy.2023.01.012

[26] Knapp, G. L., Mukherjee, T., Zuback, J. S., Wei, H. L., Palmer, T. A., De, A., & DebRoy, T. J. A. M. (2017). Building blocks for a digital twin of additive manufacturing. *Acta Materialia*, *135*, 390-399, https://doi.org/10.1016/j.actamat.2017.06.039

[27] Liu, C., Le Roux, L., Körner, C., Tabaste, O., Lacan, F., & Bigot, S. (2022). Digital twin-enabled collaborative data management for metal additive manufacturing systems. *Journal of Manufacturing Systems*, *62*, 857-874, https://doi.org/10.1016/j.jmsy.2020.05.010

[28] Yavari, R., Riensche, A., Tekerek, E., Jacquemetton, L., Halliday, H., Vandever, M., ... & Rao, P. (2021). Digitally twinned additive manufacturing: Detecting flaws in laser powder bed fusion by combining thermal simulations with in-situ meltpool sensor data. *Materials & Design*, *211*, 110167, https://doi.org/10.1016/j.matdes.2021.11016

[29] Reisch, R. T., Hauser, T., Lutz, B., Tsakpinis, A., Winter, D., Kamps, T., & Knoll, A. (2022). Context awareness in process monitoring of additive manufacturing using a digital twin. *The International Journal of Advanced Manufacturing Technology*, 1-18, https://doi.org/10.1007/s00170-021-08636-5

[30] Latsou, C., Farsi, M., & Erkoyuncu, J. A. (2023). Digital twin-enabled automated anomaly detection and bottleneck identification in complex manufacturing systems using a multi-agent approach. *Journal of Manufacturing Systems*, *67*, 242-264, https://doi.org/10.1016/j.jmsy.2023.02.008

[31] Phua, A., Davies, C. H. J., & Delaney, G. W. (2022). A digital twin hierarchy for metal additive manufacturing. *Computers in Industry*, *140*, 103667, https://doi.org/10.1016/j.compind.2022.103667

[32] Ishfaq, K., Khan, M. D. A., Khan, M. A. A., Mahmood, M. A., & Maqsood, M. A. (2023). A correlation among industry 4.0, additive manufacturing, and topology optimization: A state-of-the-art review. *The International Journal of Advanced Manufacturing Technology*, *129*(9), 3771-3797, https://doi.org/10.1007/s00170-023-12515-6

[33] Suhail, S., Malik, S. U. R., Jurdak, R., Hussain, R., Matulevičius, R., & Svetinovic, D. (2022). Towards situational aware cyber-physical systems: A security-enhancing use case of blockchain-based digital twins. *Computers in Industry*, *141*, 103699, https://doi.org/10.1016/j.compind.2022.103699

[34] Sandborn, M., Olea, C., White, J., Williams, C., Tarazaga, P. A., Sturm, L., ... & Tenney, C. (2021). Towards secure cyber-physical information association for parts. *Journal of Manufacturing Systems*, *59*, 27-41, https://doi.org/10.1016/j.jmsy.2021.01.003

[35] Guo, D., Ling, S., Li, H., Ao, D., Zhang, T., Rong, Y., & Huang, G. Q. (2020, August). A framework for personalized production based on digital twin, blockchain and additive manufacturing in the context of Industry 4.0. In *2020 IEEE 16th International Conference on Automation Science and Engineering (CASE)* (pp. 1181-1186). IEEE.

[36] Mandolla, C., Petruzzelli, A. M., Percoco, G., & Urbinati, A. (2019). Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry. *Computers in industry*, *109*, 134-152, https://doi.org/10.1016/j.compind.2019.04.011

[37] Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024). Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express*, *10 (4)*, 935-958, https://doi.org/10.1016/j.icte.2024.05.00

[38] Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J. C., Ávila, M., & Caro, A. (2024). A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artificial Intelligence Review*, *57*(8), 201, https://doi.org/10.1007/s10462-024-10805-3

[39] Jiang, Y., Wang, W., Ding, J., Lu, X., & Jing, Y. (2024). Leveraging Digital Twin Technology for Enhanced Cybersecurity in Cyber–Physical Production Systems. *Future Internet*, *16*(4), 134. https://doi.org/10.3390/fi16040134

[40] Assuad, C. S. A., Leirmo, T., & Martinsen, K. (2022). Proposed framework for flexible de-and remanufacturing systems using cyber-physical systems, additive manufacturing, and digital twins. *Procedia CIRP*, *112*, 226-231, https://doi.org/10.1016/j.procir.2022.09.076

[41] Karkaria, V., Goeckner, A., Zha, R., Chen, J., Zhang, J., Zhu, Q., ... & Chen, W. (2024). Towards a digital twin framework in additive manufacturing: Machine learning and Bayesian optimization for time series process optimization. *Journal of Manufacturing Systems*, *75*, 322-332, https://doi.org/10.1016/j.jmsy.2024.04.023

[42] Putra, M. A. P., Rachmawati, S. M., Alief, R. N., Ahakonye, L. A. C., Gohil, A., Kim, D. S., & Lee, J. M. (2023, February). Federated Learning-Enabled Digital Twin for Smart Additive Manufacturing Industry. In *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* (pp. 806-811). IEEE.

[43] Masi, M., Sellitto, G. P., Aranha, H., & Pavleska, T. (2023). Securing critical infrastructures with a cybersecurity digital twin. *Software and Systems Modeling*, *22*(2), 689-707, https://doi.org/10.1007/s10270-022-01075-0.

[44] Pirbhulal, S., Abie, H., & Shukla, A. (2022, June). Towards a novel framework for reinforcing cybersecurity using digital twins in IoT-based healthcare applications. In *2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)* (pp. 1-5). IEEE.

[45] Holmes, D., Papathanasaki, M., Maglaras, L., Ferrag, M. A., Nepal, S., & Janicke, H. (2021, September). Digital Twins and Cyber Security–solution or challenge?. In *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)* (pp. 1-8). IEEE.

[46] da Silva, A. C. F., Wagner, S., Lazebnik, E., & Traitel, E. (2022). Using a cyber digital twin for continuous automotive security requirements verification. *IEEE Software*, *40*(1), 69-76.

[47] Frank, W., Hajj, R., Robbins, A., and Das, R. (2023). Cyber digital twin: Building blocks of a secure Industry 4.0 metaverse, Deloitte Development LLC., https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-rfa-digital-twin-5x5-final.pdf

[48] Sellitto, G. P., Masi, M., Pavleska, T., & Aranha, H. (2021, November). A Cyber security digital twin for critical infrastructure protection: the intelligent transport system use case. In *IFIP Working Conference on The Practice of Enterprise Modeling* (pp. 230-244). Cham: Springer International Publishing. 10.1007/978-3-030-91279-6_16. hal-04323852

[49] Gupta, N. iwari, A.. Bukkapatnam, S. T. S and Karri, R. (2020). "Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks," in *IEEE Access*, vol. 8, pp. 47322-47333, 2020, doi: 10.1109/ACCESS.2020.2978815

[50] Sturm, L. D., Williams, C. B., Camelio, J. A., White, J., & Parker, R. (2017). Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. STL file with human subjects. *Journal of Manufacturing Systems*, *44*, 154-164, doi: 10.1016/j.jmsy.2017.05.007

[51] Rahman, S., Hossain, N. U. I., Govindan, K., Nur, F., & Bappy, M. (2021). Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chain. *CIRP Journal of manufacturing science and technology*, *35*, 911-928, https://doi.org/10.1016/j.cirpj.2021.09.008

[52] Corallo, A., Lazoi, M., Lezzi, M., & Pontrandolfo, P. (2021). Cybersecurity challenges for manufacturing systems 4.0: assessment of the business impact level. *IEEE Transactions on Engineering Management*, *70*(11), 3745-3765, doi: 10.1109/TEM.2021.3084687